

Gartner Says SAS 70 Is Not Proof of Security, Continuity or Privacy Compliance

August 16, 2010

By 2012, No Customers of Cloud Providers Will Accept SAS 70 Alone as Proof of Effective Security and Compliance

STAMFORD, Conn. — _Statement on Auditing Standards (SAS) 70 is being misused by many vendors, and often their customers and certified public accountants (CPAs), in the hosted-application, software as a service (SaaS) and cloud computing spaces, according to Gartner, Inc.

Gartner analysts said SAS 70 is too often treated by vendors and their customers as a certification "proving" security and compliance with privacy or other regulations that require enterprises to monitor their exposure to vendor risks.

"SAS 70 is basically an expensive auditing process to support compliance with financial reporting rules like the Sarbanes-Oxley Act (SOX)," said French Caldwell, research vice president at Gartner. "Chief information security officers (CISOs), compliance and risk managers, vendor managers, procurement professionals, and others involved in the purchase or sale of IT services and software need to recognize that SAS 70 is not a security, continuity or privacy compliance standard."

Published by the American Institute of Certified Public Accountants (AICPA), SAS 70 provides a service provider's auditor with guidance on how it should report on process-related risks relevant to financial statements and transaction processing. Intended for use by the customer's auditor, the result of a SAS 70 is either a Type I attestation that the processes as documented are sufficient to meet specific control objectives, or a Type II attestation, which additionally includes an on-site evaluation to determine whether the processes and controls actually function as anticipated.

"Many providers of traditional application hosting, SaaS and cloud computing are currently treating SAS 70 as if it were a form of certification, which it is not," said Jay Heiser, research vice president at Gartner. "Furthermore, some claim that SAS 70 addresses security, privacy and continuity, which is misleading. Instead, it is only a generic guideline for the preparation, procedure and format of an auditing report. SAS 70 always places the onus on the service recipient, or more precisely, on the recipient's auditor, to ensure that all controls relevant to the recipient's requirements are examined."

In its intended context of financial reporting and transaction services, buyers' auditors could reasonably be expected to know what controls are needed to meet buyers' contractual requirements, and to identify gaps, but this is not the case with alternative computing delivery models. Gartner does not consider the auditing profession as being the most appropriate provider for all forms of IT risk assessment.

"Given that SAS 70 cannot be considered as proof that an offered IT service is secure, it should be a matter of suspicion when a vendor insists that it is," Mr. Heiser said. "Vendor claims to be 'SAS 70 certified' indicate either ignorance or deception, neither of which is a good basis for trust. The only thing that can conclusively be said about having a SAS 70 Type II attestation is that an auditing firm has agreed that the service provider is effectively performing those controls that they paid the auditing firm to evaluate."

Nevertheless, Gartner analysts said a SAS 70 Type II evaluation does provide a very high degree of assurance that the examined controls are effective. The performance of controls is evaluated over a period of time; it is not just a snapshot of control effectiveness. However, customers should never assume that the provider has implemented all the appropriate controls, and they must review the controls documentation at a minimum and, ideally, review the complete evaluation report.

SAS 70 is one of several mechanisms that can be used to evaluate a service provider's control environment. Gartner recommends a mix of the following methods that can be used to supplement or serve as an alternative to SAS 70: background and reference checks; vendor self-assessment and attached evidence (evidence could include SAS 70, Payment Card Industry security assessments, self-testing, and records from other external audits and assessors); on-site audit or assessment by the enterprise's own security assessors or internal auditors and application of direct controls on the services provider, for example having vendor employees undertake the organization's ethics training and sign off on the code-of-conduct policy.

Enterprises may also want to evaluate alternative assessment standards for vendor security, compliance and risk management, such as International Organization for Standardization (ISO) standard certifications, BITS Shared Assessments (which are provided by a consortium of service providers, their customers, audit firms and other third-party assessors), SysTrust and WebTrust (which are formal security certifications that are sponsored by the AICPA and carried out by CPA-qualified auditors), and AT Section 101, which is a flexible attestation procedure sponsored by AICPA that can be used by any CPA-qualified auditor.

"Standards organizations are in the process of adapting their standards to better address the unique risk issues of cloud computing. Their efforts are iterative, and service providers, customers and auditors must ensure that the standards and assessment procedures that they adopt align with the specific cloud environment of the service provider," Mr. Caldwell said. "To ensure that vendor controls are effective for security, privacy compliance and vendor risk management, SAS 70, its successor Statement on Standards for Attestation Engagements (SSAE) 16, and other national audit standard equivalents should be supplemented with self-assessments and agreed-upon audit procedures."

Additional detail is available in the Gartner report "SAS 70 Is Not Proof of Security, Continuity or Privacy Compliance." The report is available on Gartner's website at <http://www.gartner.com/resId=1390444>